REMARKS

In response to the final Office Action mailed June 5, 2007, Applicants respectfully request entry of this amendment. Claims 1-33 and 37-39 were previously pending in this application. Claims 1, 12, 13, 18, 19, 21 and 37 have been amended. As a result, claims 1-33 and 37-39 are pending for examination with claims 1, 19, 21 and 37 being independent. No new matter has been added.

Rejections under 35 U.S.C. §112

The Office Action rejected claim 1 under 35 U.S.C. 112, second paragraph, as allegedly being incomplete. Applicants have amended claim 1.

Accordingly, withdrawal of this rejection is respectfully requested.

Rejections under 35 U.S.C. §101

The Office Action rejected claims 18 and 33 under 35 U.S.C. 101 as allegedly directed to non-statutory subject matter. Applicants have amended claims 18 and 33 to address the Examiner's concerns.

Accordingly, withdrawal of these rejections is respectfully requested.

In the specification

Applicants have amended the specification to correct two minor typographical errors.

Rejections Under 35 U.S.C. §102

The Office Action rejected claims 1-6, 9-33 and 37-39 under 35 U.S.C. 102(e) as allegedly being unpatentable over Malcolm, U.S. Patent No. 7,146,638 (hereinafter Malcolm) in view of Chakravarty, U.S. Published Patent Application No. 2004/0128545 (hereinafter Chakravarty). Applicants respectfully disagree.

I. Independent Claim 1

Claim 1, as amended, recites:

> A computer-implemented method, comprising:
>
> receiving, *by an operating system and/or an enforcement module which is associated with or is part of the operating system*, a call from an application *via a first application programming interface*, the call having parameters for a connection to an endpoint that the application desires to establish, whereby *the application explicitly communicates a request* to establish the connection; and
>
> making, *by the operating system and/or the enforcement module*, a call *via a second application programming interface* to a firewall to establish the connection in accordance with the parameters.
>
> (Emphasis added).

Malcolm is directed to controlling by a firewall program whether an application program is granted access to a wide area network (WAN), such as the Internet (Abstract). *The firewall receives the at least one access request definition from the application program* during startup of the application program or immediately prior to the intercepted access request (col. 4, lines 20-25). (Emphasis added). Specifically, *the application program will preferably provide the firewall program* with a list of Internet access requests that the application may possibly have during execution of the application (col. 6, lines 41-44).

Malcolm neither teaches nor suggests "a computer-implemented method, comprising: receiving, by an operating system and/or an enforcement module which is associated with or is part of the operating system, a call from an application via a first application programming interface, the call having parameters for a connection to an endpoint that the application desires to establish, whereby the application explicitly communicates a request to establish the connection; and making, by the operating system and/or the enforcement module, a call via a second application programming interface to a firewall to establish the connection in accordance with the parameters," as recited in claim 1.

Chakravarty is directed to dynamically controlling a set of filtering-related operations at a firewall from one or more hosts (Abstract). A host sends a command to the firewall to request the establishment of a filter rule at the firewall (page 1, ¶ 0007). The process begins with *the host monitoring one or more communication protocol command channels* (step 302). The host determines if a command has been received (step 304), and if not, it cycles until a command is detected. If the host has received a command, then the host authenticates the requester if necessary (Fig. 3; page 2, ¶ 0025). (Emphasis added).

Chakravarty does not describe "a call from an application via a first application programming interface … whereby the application explicitly communicates a request to establish the connection," as recited in claim 1. Furthermore, even though one embodiment of Chakravarty describes, with reference to Fig. 4, that *the application itself*, e.g., such as an FTP application daemon, sends the command to the firewall in order to enable a data connection before sending an FTP request (page 3, ¶ 0031), this embodiment does not describe a first and a second application programming interfaces that provide mechanisms by which firewall aware application may communicate a request to a host or edge firewall, as discussed on page 25, ¶ 0055 of the present application .

Therefore, Chakravarty neither teaches nor suggests "a computer-implemented method, comprising: receiving, by an operating system and/or an enforcement module which is associated with or is part of the operating system, a call from an application via a first application programming interface, the call having parameters for a connection to an endpoint that the application desires to establish, whereby the application explicitly communicates a request to establish the connection; and making, by the operating system and/or the enforcement module, a call via a second application programming interface to a firewall to establish the connection in accordance with the parameters," as recited in claim 1.

In view of the foregoing, claim 1 patentably distinguishes over Malcolm and Chakravarty, either alone or in combination.

Claims 2-18 depend from claim 1 and are allowable for at least the same reasons.

Accordingly, withdrawal of the rejection of claims 1-18 is respectfully requested.

II. <u>Independent Claim 19</u>

Claim 19, as amended, recites:

> A computer system comprising:
> an operating system;
> *a first application programming interface* associated with the operating system and configured and adapted to receive a call from an application, the call having parameters for a connection to an endpoint that the application desires to establish, *whereby the application explicitly communicates a request* to establish the connection; and
>
> an enforcement module associated with the operating system and called via the application programming interface and configured and adapted to:

> receive an indication from the application that the application desires to establish the connection; and
>
> make a call *via a second application programming interface* to a firewall to establish the connection in accordance with the parameters.
>
> (Emphasis added).

As discussed above, neither Malcolm nor Chakravarty teaches or suggests "a computer system comprising: an operating system; a first application programming interface associated with the operating system and configured and adapted to receive a call from an application, the call having parameters for a connection to an endpoint that the application desires to establish, whereby the application explicitly communicates a request to establish the connection; and an enforcement module associated with the operating system and called via the application programming interface and configured and adapted to: receive an indication from the application that the application desires to establish the connection; and make a call via a second application programming interface to a firewall to establish the connection in accordance with the parameters," as recited in claim 19.

In view of the foregoing, claim 19 patentably distinguishes over Malcolm and Chakravarty, either alone or in combination.

Claim 20 depends from claim 19 and is allowable for at least the same reasons.

Accordingly, withdrawal of the rejection of claims 19 and 20 is respectfully requested.

III. Independent Claim 21

Claim 21, as amended, recites:

> A computer-implemented method, comprising:
>
> receiving, *by an interception module including an application programming interface and a filter cache,* a connect attempt, a listen attempt, or a combination thereof from an application or a service;
>
> extracting, *by the interception module*, user and application or service information from the connect attempt, the listen attempt, or the combination thereof;
>
> identifying, *by the interception module*, a user and the application or the service from the user and application or service information;
>
> evaluating, *by the interception module*, the application or service information to determine if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from a plurality of policies; and

> if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from the plurality of policies, instructing, by the interception module, a firewall to create a configuration to allow the connect attempt, the listen attempt, or the combination thereof, and *storing the configuration in the filter cache*.
>
> (Emphasis added).

As discussed above, Malcolm neither teaches nor suggests "a computer-implemented method, comprising: receiving, by an interception module including an application programming interface and a filter cache, a connect attempt, a listen attempt, or a combination thereof from an application or a service; extracting, by the interception module, user and application or service information from the connect attempt, the listen attempt, or the combination thereof; identifying, by the interception module, a user and the application or the service from the user and application or service information; evaluating, by the interception module, the application or service information to determine if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from a plurality of policies; and if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from the plurality of policies, instructing, by the interception module, a firewall to create a configuration to allow the connect attempt, the listen attempt, or the combination thereof, and storing the configuration in the filter cache," as recited in claim 21.

Chakravarty describes that firewall 408 filters incoming and outgoing commands and data for various communication protocols through its filtering engine 412. Filter rule management module 416 *creates new filter rules or deletes currently active filter rules that are stored within filter rule table 418* (Fig. 4, page 3, ¶ 0029). (Emphasis added). In contrast, an interception module includes an application programming interface and a filter cache, as recited in claim 21, support for which can be found on page 31, ¶ 0070 of the present application. Further, claim 21 recites instructing, by the interception module, a firewall to create a configuration to allow the connect attempt, the listen attempt, or the combination thereof, and storing the configuration in the filter cache (support for this can be found on page 34, ¶ 0074 of the present application).

In view of the foregoing, claim 21 patentably distinguishes over Malcolm and Chakravarty, either alone or in combination.

Claims 22-33 depend from claim 21 and are allowable for at least the same reasons.

Accordingly, withdrawal of the rejection of claims 21-33 is respectfully requested.

IV. Independent Claim 37

Claim 37, as amended, recites:

> A computer system, comprising:
> a firewall; and
> an interception module including an application programming interface and a filter cache and configured and adapted to:
> intercept a request for a connect attempt, a listen attempt, or a combination thereof from an application or a service;
> extract user and application or service information from the connect attempt, the listen attempt, or the combination thereof;
> identify a user and the application or the service from the user and application or service information;
> evaluate the application or service information to determine if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from a plurality of policies; and
> if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from the plurality of policies, instructing the firewall to create a configuration to allow the connect attempt, the listen attempt, or the combination thereof, *and storing the configuration in the filter cache*. (Emphasis added).

As discussed above, neither Malcolm nor Chakravarty teaches or suggests "a computer system, comprising: a firewall; and an interception module including an application programming interface and a filter cache and configured and adapted to: intercept a request for a connect attempt, a listen attempt, or a combination thereof from an application or a service;

extract user and application or service information from the connect attempt, the listen attempt, or the combination thereof; identify a user and the application or the service from the user and application or service information; evaluate the application or service information to determine if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from a plurality of policies; and if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from the plurality of policies, instruct instructing the firewall to create a configuration to allow the connect attempt, the listen attempt, or the combination thereof, and storing the configuration in the filter cache," as recited in claim 37.

In view of the foregoing, claim 37 patentably distinguishes over Malcolm and Chakravarty, either alone or in combination.

Claims 38-39 depend from claim 37 and are allowable for at least the same reasons.

Accordingly, withdrawal of the rejection of claims 37-39 is respectfully requested.

CONCLUSION

A Notice of Allowance is respectfully requested. The Examiner is requested to call the undersigned at the telephone number listed below if this communication does not place the case in condition for allowance.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicants hereby request any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 23/2825.

Dated: August 6, 2007

Respectfully submitted,

By ______________________
James H. Morris
Registration No.: 34,681
WOLF, GREENFIELD & SACKS, P.C.
Federal Reserve Plaza
600 Atlantic Avenue
Boston, Massachusetts 02210-2206
(617) 646-8000